

# IT security

## - sharing problems and solutions

*Stephen Cummings introduces a new type of information sharing model - the WARP - and examines its role in the public sector.*

If a problem shared is a problem halved, then sharing it with a large group of people in similar circumstances to yours could reduce it significantly. Indeed, it could be solved altogether if someone else has a solution to fit your problem. This is one part of the basic thesis of the information sharing initiative led by a critically important central government organisation in the public sector IT security world - the National Infrastructure Security Coordination Centre (NISCC).

The NISCC is promoting a new concept called the WARP - Warning, Advice and Reporting Point. The idea is to bring together groups of people and organisations to pool resources for monitoring alerts and warnings, exchange advice and good practice and (safely) share experiences of incidents for the benefit of all members and ultimately the common good.

Much of this work goes under the general heading of information sharing but should not be confused with the issue of data sharing or data exchange, which is currently exercising many public sector authorities concerned with transferring information between agencies.

The WARP owes its lineage to the global Computer Emergency Response Team (CERT) network, which will be familiar to many technical IT security experts and includes the UK Government CERT, Uniras, which is now part of NISCC's Response section. There are perhaps a few hundred CERTs around the world (see [www.FIRST.org](http://www.FIRST.org)) but they generally serve fairly technical communities and the WARP programme is a way of extending this concept to a much broader audience, and, significantly, at a fraction of the cost of most CERTs.

The US Department of Homeland Security has just announced the establishment of a national CERT providing warnings and advice for home users and small businesses in particular. The USCERT's National Cyber Alert System is a large-scale warning system, aimed at a common core of needs; the WARP concept can complement such a wide-reaching system, since its focus is rather different.

A WARP is established to provide a customised, tailored service for a small community. It will monitor the wealth of sources of warnings and advisories currently available via the internet, from

vendors, CERTs, advice centres etc and filter them so that the WARP's members only receive those that are relevant. This Warning service saves each member duplicating the same work in trawling through a load of sources every day to find those of interest. The time saved by each member can alone be enough to fund the WARP's resource costs, just through a co-operative pooling of effort. The WARP model has two other major functions including the Advice service, whereby the WARP can point members to sources of advice, contacts etc (the WARP staff do not need to be technical experts themselves). More importantly, the WARP can act as a focus for the members themselves to exchange knowledge, best practice and even skills, possibly using a dedicated bulletin board.

The third element of the WARP is to provide a trusted focus for members for Reporting incidents (attacks, problems, vulnerabilities) in a safe environment where the information will be held securely. Once it has been anonymised and sanitised, it can be issued to the rest of the membership to provide timely, real and highly relevant warnings and awareness material. After all, what could possibly be more relevant to assessing and protecting against threats to your organisation, than to know that one of your fellow members (be they colleagues, competitors or neighbours) has just been attacked, and possibly even how they rebutted or recovered from the attack? You would not know who had originated the report of course, but you would know it was a real incident and it could save your own organisation considerable embarrassment, expense, or worse.

*A WARP will monitor the wealth of sources of warnings and advisories currently available via the internet, from vendors, CERTs, advice centres – WARP members will only receive those that are relevant.*

Naturally, there are lots of serious issues to be considered when joining or setting up a WARP and the concept is still relatively new and needs working through in different situations. NISCC's Information Sharing programme has gone a long way in addressing these issues however, and has set up a number of pilot schemes to trial and develop the WARP model, with support from the Central Sponsor for Information Assurance. The first WARP was established in partnership with London Connects, serving the London Borough councils and it has done a lot of work in defining and developing these services. A second WARP is due to be launched soon, serving the local authorities in Kent, championed by Kent Connects, and will be part of their 'Secure Kent' IT Security initiative.

A major step forward is expected in the next few months with the first issue of the WARP Toolbox. This will contain a collection of key information about how to establish and run a WARP. The Toolbox will include material on: business cases, resources, funding, service definitions, requirements analysis, security policy, NDAs and many other items, with a particular focus on delivering the three key service packages: the Filtered Warning and Advisory Service; Good Practice and Advice

Brokering Service; and the Reporting and Trusted Sharing Service. We are also currently trialling a software suite for implementing the Filtered Warning service, which will be made available as soon as possible. This software is being specially developed for the WARP programme by Microsoft at their own cost and they are one of a number of prestigious companies providing real and highly valued support to NISCC's WARP initiative.

The WARP Toolbox will be supplemented as new items are developed and as lessons are learned from the pilot schemes and it will be freely available from NISCC to anyone who wants to set up their own WARP. The intention is that WARPs will be established by all sorts of communities, within large organisations, for small business and consumer groups, in local authorities and by interest groups. The WARP concept is flexible, versatile and low-cost and our aim is to encourage the establishment of a network of WARPs, supporting each other in conjunction with CERTs.

NISCC wants to be linked into this network, to have access to more incident reporting and to have a sophisticated channel for disseminating warnings and advisories more effectively. The very existence of WARPs, however, will serve to improve the awareness, education and protection of all IT users who receive their services, and that improves the cyber environment for all of us, including the UK's CNI. Much has already been achieved with very modest resources, but with the continuing help of partners in industry and the public sector, the prospects are very encouraging.

Stephen Cummings, Director NISCC  
[www.niscc.gov.uk](http://www.niscc.gov.uk)  
[sharing@niscc.gov.uk](mailto:sharing@niscc.gov.uk)  
[www.USCERT.gov](http://www.USCERT.gov)  
[www.lcwarp.org.uk](http://www.lcwarp.org.uk)